

Evaluation Scoring

Remember to be consistent with scoring methodology

0	Did not provide an answer
2	Incoherent, communicates a lack of understanding and/or capability
4	Marginal, communicates a weak knowledge, understanding, and/or capability
6	Average, communicates an average knowledge, understanding, and/or capability
8	Good, communicates that they are good at what they do and have a good understanding
10	Excellent, communicates that they are not just good, but provide value added services and capabilities that may exceed expectations

Give one score for each question - the average of all scores will be the total points awarded for the interview.

K689 - Security Assessment Services							
Vendor: Emagined							
Interview Total 10 pts							
Question 1	Many of the state agencies and local governments we work with have thick client applications that we test. Can you describe your experience with penetration testing thick client applications?						
Score	0-no answer	2-lack of understanding	4-Marginal	6-Average	8-Good	10-Excellent	Evaluator Score
							10
Question 2	Our engagements can include testing of SCADA systems. In some cases this testing must be done in production on critical systems such as water or sewer treatment plants. Can you describe your penetration testing experience with SCADA systems? What are some of the key questions you would have for the client to ensure a smooth valuable test?						
Score	0-no answer	2-lack of understanding	4-Marginal	6-Average	8-Good	10-Excellent	Evaluator Score
							8
Question 3	Our engagements sometimes include testing mainframes. These would typically be legacy applications that support core or enterprise functions, and therefore may not be as stable or robust as more modern applications. Can you describe your experience with penetration testing mainframes? What are some of the key pieces of information you would want from the client to ensure a smooth and valuable test of a mainframe?						
Score	0-no answer	2-lack of understanding	4-Marginal	6-Average	8-Good	10-Excellent	Evaluator Score
							8
Question 4	Our engagements sometimes include mobile applications? Can you describe your experience with penetration testing mobile systems? What are some of the key questions you would have for the client to ensure a smooth and valuable test?						
Score	0-no answer	2-lack of understanding	4-Marginal	6-Average	8-Good	10-Excellent	Evaluator Score
							6
Question 5							
Score	0-no answer	2-lack of understanding	4-Marginal	6-Average	8-Good	10-Excellent	Evaluator Score
							8
Question 6	From time to time we need to have more than one penetration testing engagement going simultaneously- with each engagement likely having internal and external testing with approximately 4-6 applications and network testing. Would your firm be able to staff this? If so, how much lead time would your firm require? How many penetration staff would you be able to commit to each engagement? How long would it take your staff to complete a typical penetration test of this size?						
Score	0-no answer	2-lack of understanding	4-Marginal	6-Average	8-Good	10-Excellent	Evaluator Score
							8
Question 7	Communication is an important part of penetration testing work, especially because the systems we test are not managed by SAO, but rather our auditees. Can you tell us about any experience you have testing a third-party application, for example a vendor for your direct client? What type of communication challenges did you face? How did you overcome those challenges?						
Score	0-no answer	2-lack of understanding	4-Marginal	6-Average	8-Good	10-Excellent	Evaluator Score
							10
Average Score	8.29						

Vendor: KPMG							
Interview Total 10 pts							
Question 1	Many of the state agencies and local governments we work with have thick client applications that we test. Can you describe your experience with penetration testing thick client applications?						
Score	0-no answer	2-lack of understanding	4-Marginal	6-Average	8-Good	10-Excellent	Evaluator Score
							10
Question 2	Our engagements can include testing of SCADA systems. In some cases this testing must be done in production on critical systems such as water or sewer treatment plants. Can you describe your penetration testing experience with SCADA systems? What are some of the key questions you would have for the client to ensure a smooth valuable test?						
Score	0-no answer	2-lack of understanding	4-Marginal	6-Average	8-Good	10-Excellent	Evaluator Score
							8
Question 3	Our engagements sometimes include testing mainframes. These would typically be legacy applications that support core or enterprise functions, and therefore may not be as stable or robust as more modern applications. Can you describe your experience with penetration testing mainframes? What are some of the key pieces of information you would want from the client to ensure a smooth and valuable test of a mainframe?						
Score	0-no answer	2-lack of understanding	4-Marginal	6-Average	8-Good	10-Excellent	Evaluator Score
							8
Question 4	Our engagements sometimes include mobile applications? Can you describe your experience with penetration testing mobile systems? What are some of the key questions you would have for the client to ensure a smooth and valuable test?						
Score	0-no answer	2-lack of understanding	4-Marginal	6-Average	8-Good	10-Excellent	Evaluator Score
							8
Question 5	Can you describe a time when something went wrong during a prior penetration testing engagement? How did you find out something went wrong? How did you respond or correct the situation? What lessons were learned from that event?						
Score	0-no answer	2-lack of understanding	4-Marginal	6-Average	8-Good	10-Excellent	Evaluator Score
							8
Question 6	From time to time we need to have more than one penetration testing engagement going simultaneously- with each engagement likely having internal and external testing with approximately 4-6 applications and network testing. Would your firm be able to staff this? If so, how much lead time would your firm require? How many penetration staff would you be able to commit to each engagement? How long would it take your staff to complete a typical penetration test of this size?						
Score	0-no answer	2-lack of understanding	4-Marginal	6-Average	8-Good	10-Excellent	Evaluator Score
							4
Question 7	Communication is an important part of penetration testing work, especially because the systems we test are not managed by SAO, but rather our auditees. Can you tell us about any experience you have testing a third-party application, for example a vendor for your direct client? What type of communication challenges did you face? How did you overcome those challenges?						
Score	0-no answer	2-lack of understanding	4-Marginal	6-Average	8-Good	10-Excellent	Evaluator Score
							8
Average Score	7.71						

Vendor: Online							
K689 - Security Assessment Services							
Interview Total 10 pts							
Question 1	Many of the state agencies and local governments we work with have thick client applications that we test. Can you describe your experience with penetration testing thick client applications?						
Score	0-no answer	2-lack of understanding	4-Marginal	6-Average	8-Good	10-Excellent	Evaluator Score
							10
Question 2	Our engagements can include testing of SCADA systems. In some cases this testing must be done in production on critical systems such as water or sewer treatment plants. Can you describe your penetration testing experience with SCADA systems? What are some of the key questions you would have for the client to ensure a smooth valuable test?						
Score	0-no answer	2-lack of understanding	4-Marginal	6-Average	8-Good	10-Excellent	Evaluator Score
							10
Question 3	Our engagements sometimes include testing mainframes. These would typically be legacy applications that support core or enterprise functions, and therefore may not be as stable or robust as more modern applications. Can you describe your experience with penetration testing mainframes? What are some of the key pieces of information you would want from the client to ensure a smooth and valuable test of a mainframe?						
Score	0-no answer	2-lack of understanding	4-Marginal	6-Average	8-Good	10-Excellent	Evaluator Score
							8
Question 4	Our engagements sometimes include mobile applications? Can you describe your experience with penetration testing mobile systems? What are some of the key questions you would have for the client to ensure a smooth and valuable test?						
Score	0-no answer	2-lack of understanding	4-Marginal	6-Average	8-Good	10-Excellent	Evaluator Score
							10
Question 5	Can you describe a time when something went wrong during a prior penetration testing engagement? How did you find out something went wrong? How did you respond or correct the situation? What lessons were learned from that event?						
Score	0-no answer	2-lack of understanding	4-Marginal	6-Average	8-Good	10-Excellent	Evaluator Score
							8
Question 6	From time to time we need to have more than one penetration testing engagement going simultaneously- with each engagement likely having internal and external testing with approximately 4-6 applications and network testing. Would your firm be able to staff this? If so, how much lead time would your firm require? How many penetration staff would you be able to commit to each engagement? How long would it take your staff to complete a typical penetration test of this size?						
Score	0-no answer	2-lack of understanding	4-Marginal	6-Average	8-Good	10-Excellent	Evaluator Score
							10
Question 7	Communication is an important part of penetration testing work, especially because the systems we test are not managed by SAO, but rather our auditees. Can you tell us about any experience you have testing a third-party application, for example a vendor for your direct client? What type of communication challenges did you face? How did you overcome those challenges?						
Score	0-no answer	2-lack of understanding	4-Marginal	6-Average	8-Good	10-Excellent	Evaluator Score
							10
Average Score	9.43						

K689 - Security Assessment Services							
Vendor: SAC		Interview Total 10 pts					
Question 1	Many of the state agencies and local governments we work with have thick client applications that we test. Can you describe your experience with penetration testing thick client applications? What are some of the key pieces of information you would want from the client to ensure a smooth and valuable test of a thick client?						
Score	0-no answer	2-lack of understanding	4-Marginal	6-Average	8-Good	10-Excellent	Evaluator Score
							10
Question 2	Our engagements can include testing of SCADA systems. In some cases this testing must be done in production on critical systems such as water or sewer treatment plants. Can you describe your penetration testing experience with SCADA systems? What are some of the key questions you would have for the client to ensure a smooth valuable test?						
Score	0-no answer	2-lack of understanding	4-Marginal	6-Average	8-Good	10-Excellent	Evaluator Score
							8
Question 3	Our engagements sometimes include testing mainframes. These would typically be legacy applications that support core or enterprise functions, and therefore may not be as stable or robust as more modern applications. Can you describe your experience with penetration testing mainframes? What are some of the key pieces of information you would want from the client to ensure a smooth and valuable test of a mainframe?						
Score	0-no answer	2-lack of understanding	4-Marginal	6-Average	8-Good	10-Excellent	Evaluator Score
							8
Question 4	Our engagements sometimes include mobile applications? Can you describe your experience with penetration testing mobile systems? What are some of the key questions you would have for the client to ensure a smooth and valuable test?						
Score	0-no answer	2-lack of understanding	4-Marginal	6-Average	8-Good	10-Excellent	Evaluator Score
							10
Question 5	Can you describe a time when something went wrong during a prior penetration testing engagement? How did you find out something went wrong? How did you respond or correct the situation? What lessons were learned from that event?						
Score	0-no answer	2-lack of understanding	4-Marginal	6-Average	8-Good	10-Excellent	Evaluator Score
			Vague answer				4
Question 6	From time to time we need to have more than one penetration testing engagement going simultaneously- with each engagement likely having internal and external testing with approximately 4-6 applications and network testing. Would your firm be able to staff this? If so, how much lead time would your firm require? How many penetration staff would you be able to commit to each engagement? How long would it take your staff to complete a typical penetration test of this size?						
Score	0-no answer	2-lack of understanding	4-Marginal	6-Average	8-Good	10-Excellent	Evaluator Score
							10
Question 7	Communication is an important part of penetration testing work, especially because the systems we test are not managed by SAO, but rather our auditees. Can you tell us about any experience you have testing a third-party application, for example a vendor for your direct client? What type of communication challenges did you face? How did you overcome those challenges?						
Score	0-no answer	2-lack of understanding	4-Marginal	6-Average	8-Good	10-Excellent	Evaluator Score
							10
Average Score	8.57						

Vendor: Soteria							Notes
Interview Total 10 pts							
Question 1 Score	Many of the state agencies and local governments we work with have thick client applications that we test. Can you describe your experience with penetration testing thick client applications? What are some of the key pieces of information you would want from the client to ensure a smooth and valuable test of a thick client?						Excellent explanation from one of the lead testers in regards to how they handle the scoping to gather all the necessary information as well as an explanation for their scoping and some of their
	0-no answer	2-lack of understanding	4-Marginal	6-Average	8-Good	10-Excellent	
							10
Question 2 Score	Our engagements can include testing of SCADA systems. In some cases this testing must be done in production on critical systems such as water or sewer treatment plants. Can you describe your penetration testing experience with SCADA systems? What are some of the key questions you would have for the client to ensure a smooth valuable test?						
	0-no answer	2-lack of understanding	4-Marginal	6-Average	8-Good	10-Excellent	
							10
Question 3 Score	Our engagements sometimes include testing mainframes. These would typically be legacy applications that support core or enterprise functions, and therefore may not be as stable or robust as more modern applications. Can you describe your experience with penetration testing mainframes? What are some of the key pieces of information you would want from the client to ensure a smooth and valuable test of a mainframe?						
	0-no answer	2-lack of understanding	4-Marginal	6-Average	8-Good	10-Excellent	
							8
Question 4 Score	Our engagements sometimes include mobile applications? Can you describe your experience with penetration testing mobile systems? What are some of the key questions you would have for the client to ensure a smooth and valuable test?						
	0-no answer	2-lack of understanding	4-Marginal	6-Average	8-Good	10-Excellent	
							8
Question 5 Score	Can you describe a time when something went wrong during a prior penetration testing engagement? How did you find out something went wrong? How did you respond or correct the situation? What lessons were learned from that event?						
	0-no answer	2-lack of understanding	4-Marginal	6-Average	8-Good	10-Excellent	
							10
Question 6 Score	From time to time we need to have more than one penetration testing engagement going simultaneously- with each engagement likely having internal and external testing with approximately 4-6 applications and network testing. Would your firm be able to staff this? If so, how much lead time would your firm require? How many penetration staff would you be able to commit to each engagement? How long would it take your staff to complete a typical penetration test of this size?						
	0-no answer	2-lack of understanding	4-Marginal	6-Average	8-Good	10-Excellent	
							8
Question 7 Score	Communication is an important part of penetration testing work, especially because the systems we test are not managed by SAO, but rather our auditees. Can you tell us about any experience you have testing a third-party application, for example a vendor for your direct client? What type of communication challenges did you face? How did you overcome those challenges?						
	0-no answer	2-lack of understanding	4-Marginal	6-Average	8-Good	10-Excellent	
							10
Average Score	9.14						